



9110-9P

**DEPARTMENT OF HOMELAND SECURITY**

**[Docket No. CISA-2019-0014]**

**Notice of President's National Security Telecommunications  
Advisory Committee Meeting**

**AGENCY:** Cybersecurity and Infrastructure Security Agency  
(CISA), Department of Homeland Security (DHS).

**ACTION:** Notice of Federal Advisory Committee Act (FACA)  
meeting; request for comments.

**SUMMARY:** CISA is publishing this notice to announce the  
following President's National Security Telecommunications  
Advisory Committee (NSTAC) meeting. This meeting will be  
partially closed to the public.

**DATES:** *Meeting Registration:* Registration to attend the  
meeting is required and must be received no later than 5:00  
p.m. Eastern Time (ET) on November 7, 2019. Due to limited  
seating, requests to attend in person will be accepted and  
processed in the order in which they are received.

*Speaker Registration:* Registration to speak during  
the meeting's public comment period must be received no  
later than 5:00 p.m. ET on November 7, 2019.

*Written Comments:* Written comments must be received  
no later than 5:00 p.m. ET on November 7, 2019.

*Meeting Date:* The NSTAC will meet on November 14, 2019 from 9:30 a.m. to 3:45 p.m. ET. The meeting may close early if the committee has completed its business.

**ADDRESSES:** The November 2019 NSTAC Meeting's open session will be held at the Eisenhower Executive Office Building, 1650 Pennsylvania Ave NW, Washington, DC.

*Meeting Registration:* To register, for information on services for individuals with disabilities, or to request special assistance to participate, please email NSTAC@hq.dhs.gov by 5:00 p.m. ET on November 7, 2019.

*Include "November 2019 NSTAC Meeting Registration" in the subject line of the message.*

*Comments:* Members of the public are invited to provide comment on the issues that will be considered by the committee as listed in the SUPPLEMENTARY INFORMATION section below. Associated materials that participants may discuss during the meeting will be available at [www.dhs.gov/cisa/national-security-telecommunications-advisory-committee](http://www.dhs.gov/cisa/national-security-telecommunications-advisory-committee) for review as of October 30, 2019. Comments may be submitted by 5:00 p.m. ET on November 7, 2019 and must be identified by Docket Number CISA-2019-

0014. Comments may be submitted by one of the following methods:

- *Federal eRulemaking Portal: [www.regulations.gov](http://www.regulations.gov).*

Please follow the instructions for submitting written comments.

- *Email: [NSTAC@hq.dhs.gov](mailto:NSTAC@hq.dhs.gov). Include the Docket Number CISA-2019-0014 in the subject line of the email.*

*Instructions:* All submissions received must include the words "Department of Homeland Security" and the Docket Number for this action. Comments received will be posted without alteration at [www.regulations.gov](http://www.regulations.gov), including any personal information provided.

*Docket:* For access to the docket and comments received by the NSTAC, please go to [www.regulations.gov](http://www.regulations.gov) and enter docket number CISA-2019-0014.

A public comment period will be held during the meeting from 3:00 p.m.-3:30 p.m. ET. Speakers who wish to participate in the public comment period must register by emailing [NSTAC@hq.dhs.gov](mailto:NSTAC@hq.dhs.gov). Speakers are requested to limit their comments to three minutes and will speak in order of registration. Please note that the public comment period may end before the time indicated, following the last request for comments.

**FOR FURTHER INFORMATION CONTACT:** Helen Jackson, 703-705-6276, [helen.jackson@cisa.dhs.gov](mailto:helen.jackson@cisa.dhs.gov).

**SUPPLEMENTARY INFORMATION:** The NSTAC was established by E.O. 12382, 47 FR 40531 (September 13, 1982), as amended and continued under the authority of E.O. 13889, dated September 27, 2019. Notice of this meeting is given under the Federal Advisory Committee Act (FACA), 5 U.S.C. Appendix (Pub. L. 92-463). The NSTAC advises the President on matters related to national security and emergency preparedness (NS/EP) telecommunications and cybersecurity policy.

**Agenda:** The NSTAC will meet in an open session on Thursday, November 14, 2019, to discuss current priorities related to NS/EP communications as well as cybersecurity.

Specifically, discussions with senior-level Government Stakeholders will focus on the importance of software defined networking as well as the challenges industry faces with regards to the Information and Communications Technology (ICT) supply chain. Additionally, members will receive an update regarding government progress towards recent NSTAC recommendations.

The committee will also meet in a closed session from 9:30 a.m. to 12:00 p.m. to receive a classified briefing on cybersecurity threats related to 5G and ICT supply chain

and discuss future studies based on the Government's NS/EP priorities and perceived vulnerabilities.

Basis for Closure: In accordance with section 10(d) of FACA and 5 U.S.C. 552b(c)(1) and (9)(B), *The Government in the Sunshine Act*, it has been determined that two agenda items require closure, as the disclosure of the information that will be discussed would not be in the public interest.

The first item is a classified threat briefing, which will provide NSTAC members with issues and concerns surrounding 5G and ICT supply chain. Disclosure of potential vulnerabilities and mitigation techniques is a threat to the Nation's cybersecurity posture since adversaries could use this information to compromise commercial and Government networks. This briefing will be classified at the top secret/sensitive compartmented information level, thereby exempting disclosure of the content by statute. The second agenda item, the discussion of potential NSTAC study topics, will address areas of critical cybersecurity vulnerabilities and priorities for Government. Government officials will share data with NSTAC members on initiatives, assessments, and future security requirements across public and private sector networks. The information will include specific vulnerabilities within cyberspace that affect the United States' ICT

infrastructures and proposed mitigation strategies. The premature disclosure of this information to the public would be likely to significantly frustrate implementation of a proposed agency action. Therefore, this portion of the meeting is required to be closed pursuant to section 10(d) of FACA and 5 U.S.C. 552b(c)(1) and (9)(B).

Dated: October 24, 2019.

**Helen Jackson,**

*Designated Federal Officer,*

*National Security Telecommunications Advisory Committee,*

*Cybersecurity and Infrastructure Security Agency,*

*Department of Homeland Security.*

[FR Doc. 2019-23779 Filed: 10/30/2019 8:45 am; Publication Date: 10/31/2019]